computing@computingonline.net
www.computingonline.net

Print ISSN 1727-6209
On-line ISSN 2312-5381
International Journal of Computing

COMPUTATIONAL INTELLIGENCE FOR BIOMETRIC APPLICATIONS: A SURVEY

**Ruggero Donida Labati, Angelo Genovese, Enrique Muñoz,
Vincenzo Piuri, Fabio Scotti, Gianluca Sforza**

Department of Computer Science
Università degli Studi di Milano
via Bramante 65, I-26013 Crema (CR)
{firstname.lastname}@unimi.it

Abstract: Biometric systems consist of devices, procedures, and algorithms used to recognize people based on their physiological or behavioral features, known as biometric traits. Computational Intelligence (CI) approaches are widely adopted in establishing identity based on biometrics and also to overcome non-idealities typically present in the samples. Typical areas of use of CI techniques include acquisition, segmentation, quality assessment, enhancement, feature extraction, matching, classification, multibiometric fusion, score normalization, antispoofing, and privacy protection. In this context, CI plays an important role in performing complex non-linear computations by creating models from the training data. These approaches are based on supervised as well as unsupervised training techniques. This work presents computational intelligence techniques applied to biometrics, from both theoretical and application points of view.

Keywords: Biometrics, Computational Intelligence, Neural Networks, Fingerprint, Iris, Face.

1. INTRODUCTION

Biometrics is the discipline that performs the recognition of the individuals based on their physiological or behavioral characteristics, called biometric traits, rather than using something known or possessed, such as passwords or tokens (e.g., ATM card). Biometric traits are considered to be unique for each individual, cannot be forgotten or stolen, and are difficult to counterfeit [1]. These aspects lead to an increased confidence that the person is actually who he claims to be.

Biometric traits can be divided into physiological, behavioral, or soft biometric traits. Physiological traits consist in features typical of the body of the individual, such as the fingerprint, the iris, or the face. Behavioral traits are related to actions performed by the individual, such as the gait, signature, or voice. Lastly, soft biometric traits consist in features that present reduced unicity, distinctiveness, and permanence with respect to physiological and behavioral traits. Example of soft biometric traits are the height, weight, and color of the clothes [1].

Biometric systems include the devices, procedures, and algorithms used to compare the biometric traits of individuals, in order to determine if they belong to the same person, and are typically based on six steps (Figure 1): i) acquisition; ii) segmentation; iii) quality assessment; iv) enhancement; v) feature extraction; vi) matching.

In the acquisition phase, a specific procedure is used to capture a sample of the biometric trait in a digital format. For example, the user presses the finger on a surface and the system collects the fingerprint image. The sample is then segmented in order to keep only the region containing the biometric information, and the system performs a quality assessment to determine if the sample is correctly captured and has sufficient quality to be further processed. Then, an enhancement step is used in order to increase the sample quality, subsequently the distinctive features are extracted and stored in a template, and the template is matched with a previously enrolled template, in order to determine if they belong to the same person [2, 3].

As an additional step, the biometric system may use a biometric classification to reduce the computational time by matching only the templates belonging to the same class. For example, fingerprints are classified into five classes considering general features of their pattern [4].

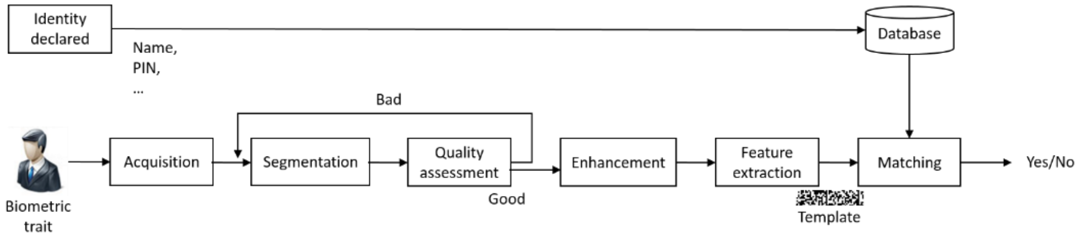

Figure 1 - Outline of a biometric recognition system.

Moreover, multibiometric systems and score normalization techniques can be used in order to increase the accuracy of biometric recognition, while antispoofing methods are used to discard counterfeit biometric samples, and privacy protection techniques are implemented to ensure the confidentiality of biometric data.

This work presents the most recent Computational Intelligence (CI) techniques from biometric recognition, from both theoretical and application points of view. The paper is structured as follows: Section 2 briefly discusses CI methods and Section 3 introduces the CI methods for biometric recognition. Section 4 summarizes the work and presents some future trends.

2. AN INTRODUCTION TO COMPUTATIONAL INTELLIGENCE

Computational Intelligence can be defined as the set of flexible and adaptive methods and mechanisms that facilitate intelligent behavior in complex and dynamic environments [5]. In fact, CI methods can work on incomplete or noise-affected data for obtaining approximate and robust solutions, with limited computational complexity. For these reasons, CI techniques are often used in biometric systems, where the biometric samples extracted from an individual are never exactly the same, thus making it necessary to use noise-robust matching methods.

In this section, we introduce the most used CI techniques in the field of biometrics, such as neural networks, kernel methods and fuzzy systems.

Neural networks were initially designed as massively parallel models suited to capture and reproduce the activities and behaviors of the human brain [6]. They offer many benefits and useful properties, such as non-linearity, adaptability, and fault tolerance [7]. Their structure is generally represented as a directed graph, where the nodes (neurons) are processing units and the links (synapses) are interactions among neurons. The topology of the interconnections defines the order of the propagation of the information among the neurons. In the literature, there are many topology proposals, such as multilayer feed-forward neural networks, recurrent neural networks, Hopfield networks or self-organizing maps. Moreover, Convolutional Neural Networks (CNN) and autoencoder neural networks are used in deep learning methods. In biometrics, neural networks are generally used for quality estimation, matching or liveness detection.

Kernel methods, on the other hand, are a family of pattern analysis algorithms that use kernels to perform a non-linear projection of data into a high-dimensional space that facilitates the learning task. The most popular kernel methods are Support Vector Machines (SVM), which have the advantages of a learning process based on the optimization of a convex surface, avoiding the stagnation in local optima, and they require the tuning of a limited number of parameters [8]. In the field of biometrics, kernel methods are mainly used for biometric fusion, matching or quality estimation.

Lastly, fuzzy systems study the imprecision and uncertainty, and the definition of methods that permit to deal with them [9]. In particular, fuzzy systems offer the advantages of using linguistic concepts, robustness against imprecise or contradictory inputs, the adaptation to conflicting objectives or the easy modification of knowledge bases. Based on these characteristics, fuzzy systems applications in biometric recognition include methods for biometric matching and fusion.

3. COMPUTATIONAL INTELLIGENCE IN BIOMETRIC RECOGNITION

In this section, we describe the most recent CI-based approaches in the literature for each step of the biometric recognition. In particular, we present the most relevant problems and the main techniques used to cope with them, with a specific focus on the most common biometric traits, such as the face, fingerprint, and iris. A summary of the considered CI methods in biometrics is presented in **Error! Reference source not found.Error! Reference source not found.**.

3.1. ACQUISITION

The acquisition of the biometric sample is the first step in the recognition process, and is performed with the aid of biometric sensors (e.g., optical scanners for fingerprints, digital cameras for the face). In this step, CI can be used for a more robust and adaptive acquisition, by performing a self-calibration [10] of the devices, or an automatic detection of errors in the tuning process [6].

Table 1 - Summary of CI-based methods for each biometric step

	CI-based method		
Biometric operation	Neural networks	Kernel methods	Fuzzy systems
Acquisition	Self-calibration [10] Error detection [6]	-	-
Segmentation	Trait location [11] [12] [13] Landmark location [14] Threshold adaptation [15] [16] Boundary detection [17] Occlusion detection [18] [19]	Trait location [13] Landmark location [14] Boundary detection [20]	Trait location [13] Threshold adaptation [21] Boundary detection [22]
Quality assessment	Problem detection [23] [24] Quality assessment [25] [26] [27] [28]	Illumination quality [29] Quality assessment [30] [31] [32] Focus assessment [33]	-
Enhancement	Image reconstruction [34] Artifact elimination [35] Rotation correction [36]	-	-
Feature extraction	Robust feature extraction [37] [38] [39] [40] [41] Candidate filtering [42] Automatic deep learning features [43] [44] [45]	-	-
Matching	Trait alignment [46] Robust matching [47] Uncontrolled scenarios [48]	Trait alignment [49] Robust matching [50] Uncontrolled scenarios [51]	Robust matching [50] [52] Coping with distortions [53]
Classification	Computational time optimization [54] [55] [56] [57] [58]	Computational time optimization [54]	-
Multibiometric fusion	Sensor-level fusion [59]	Feature-level fusion [60] Score-level fusion [61]	Score-level fusion [62]
Score normalization	-	Optimization of impostor and genuine distributions [63] [64]	-
Antispoofing	Detection of physiological features [65]	Motion analysis [66] [67] [68] Texture analysis [69] Detection of physiological features [70] [71]	Detection of physiological features [72]
Privacy protection	Trait encryption [73] [74]	Trait encryption [73]	-

3.2 SEGMENTATION

The segmentation step separates the actual biometric trait from the background. This step is critical to guarantee a high recognition rate, and can be influenced by many factors, such as changes in image orientation, occlusions or varying illumination conditions. In addition, each trait can have specific segmentation challenges.

In face recognition, the segmentation step separates the face from the background, and can be complicated by changes in pose, facial expression or background variations [75]. In this context, neural networks are among the most popular techniques for face segmentation [11, 12], also in combination with fuzzy logic and SVMs [13]. Moreover, it may be also necessary to locate the facial landmarks [4]. Many techniques used for these purpose are based on SVMs or neural networks [14].

In the case of fingerprint recognition, the segmentation of the ridge pattern allows to avoid the extraction of spurious features from the background. This process can be difficult because the fingerprint is a striated pattern, and the use of global or local thresholds can obtain unsatisfactory results [4]. For this reason, neural networks [15, 16] and fuzzy techniques [21] have been proposed to improve the segmentation accuracy.

The case of iris segmentation is particularly difficult, since the iris is a small moving area, often occluded by the eyelids and eyelashes. Moreover, off-axis gazes or high distances can pose additional challenges [76], resulting in the segmentation as the most computationally demanding step in iris recognition. For this reason, iris boundary detection has often been approached using CI techniques, like fuzzy systems [22], kernel methods [20], or neural networks [17]. In addition, neural networks have been applied to detect occlusions such as reflections, eyelids, and eyelashes [18, 19].

3.3 QUALITY ASSESSMENT

The quality of biometric samples has a great impact on the performance of biometric systems [23, 77]. Quality metrics are then used to predict the recognition performance of a sample, so that higher-quality values correspond to a better recognition of the individuals [78]. However, estimating the correspondence between a sample and its recognition capability can be complex. For this reason, CI techniques have been often used in this context to learn the relation between a sample and its quality.

In face recognition, some works use general image properties, such as contrast, sharpness, and illumination intensity in order to assess the quality of the image. In particular, kernel methods are used in [29] to predict illumination quality, in [30] to link the quality to the uniqueness of the sample, and in [31] to assess the quality based on holistic face features.

In fingerprint recognition, poor skin conditions, dirty fingers, inexperience of the user, or ergonomic factors can degrade sample quality [23]. In this context, the most commonly used quality assessment methods, NFIQ and NFIQ 2.0, use feedforward neural networks [25] and self-organizing maps [26]. Neural networks have been also used to isolate the problem that caused a low-quality fingerprint sample [23], and to analyze the quality of touchless [27] and 3D fingerprint images [28].

In iris recognition systems, occlusions, off-angle gaze, environmental and camera effects (e.g., out-of-focus blur) can influence the quality of the iris image [24]. CI techniques such as SVMs have been used to analyze local patterns [32] and to measure the focus [33], while neural networks have been used to detect multiple problems at the same time [24].

3.4 ENHANCEMENT

CI techniques have been applied for the enhancement of biometric samples, especially in the case of fingerprint images. In fact, variations in the position and exerted pressure of the finger on the sensor can cause regions of the image where the details of the fingerprint, specifically the ridges and valleys, are not clearly defined. For this reason, a preprocessing step is used to level out the quality of the image before extracting the features [4].

Traditionally, fingerprint enhancement is performed in three steps: i) ridge enhancement; ii) image binarization; iii) ridge thinning. In particular, the method proposed in [34] uses a Convolutional Deep Belief Network (CDBN) trained on fingerprint images, selected from a database based on their superior quality. The network then works directly on the pixels of the fingerprint image and performs the enhancement by reconstructing characteristics similar to the ones of the images used in the training phase. Moreover, Pulse-Coupled Neural Networks (PCNNs) are used in the method described in [35] to perform ridge thinning. In order to avoid artifacts often created by thinning algorithms, the network is trained with a set of correct thinning results. Lastly, the method proposed in [36] performs the correction of perspective and rotation effects in touchless fingerprint images, by using neural networks to estimate the rotation of the sample with respect to an enrolled template, and synthetic three-dimensional models to compensate for the rotation.

3.5 FEATURE EXTRACTION

The feature extraction process has the purpose of extracting the most distinctive characteristics of the biometric trait, which are then matched in order to perform the identity comparison.

In face recognition, the method described in [43] uses supervised autoencoders in order to extract robust features from images subject to variations in pose, expression, and illumination, in order to recognize individuals using a single image for individual in the training phase. Similar methods based on Deep Learning techniques have been proposed for extracting features from unconstrained face images captured from multimedia applications [44], and in the wild [45]. Moreover, the method proposed in [39] computes a 3-D representation of the face from a single image using RBF neural networks, trained using several 2-D images coupled with the corresponding 3-D model.

In fingerprint recognition systems, the most used features include the orientation of the ridges and the positions of singular points, minutiae points, sweat pores, and incipient ridges [4]. Feedforward neural networks are used in [37] to detect the position of the Principal Singular Point (PSP) in both touch-based and touchless images. The approach extracts a list of candidate points, then uses a trained neural network to select the PSP among the candidates. Moreover, the method described in [38] uses CNNs, trained using noise-corrupted rolled images, to extract the orientation of the ridges from latent fingerprint images. Lastly, the method described in [42] extracts the positions of sweat pores from touchless fingerprint images. The approach uses feedforward neural networks trained with features extracted from local image regions centered on manually-estimated positions of the pores.

In iris recognition, a method based on a combination of Haar Wavelet decomposition and neural networks for extracting robust feature from iris images captured in unconstrained conditions is proposed in [40]. Moreover, the method proposed in [41] applies unsupervised PCNNs on iris samples to output binary images, which are then matched using the Hamming distance.

3.6 MATCHING

The matching process compares the features obtained from the live sample with a previously enrolled template, to check if they correspond to the same person. The result of this process is a similarity score. Finally, a threshold is used to determine the acceptance or rejection of the matching. Matching algorithms have to deal with variations of the extracted features [4], which may appear as a result of changes in the trait (e.g., disease, aging), different presentation (orientation, pose) or noise (different illumination, blur). CI techniques are robust against imprecision and uncertainty, and for that reason have been frequently used for matching.

In face recognition, the first step in matching is the alignment of the faces, which has a great impact in the recognition performance. The application of neural networks [46] or SVM [49] to this problem has obtained very accurate results. Once the faces have been aligned, the extracted features are matched using methods such as deep learning [47] or fuzzy SVMs [50].

In fingerprint recognition, biometric matching is a challenging problem, especially for low-quality images and latent fingerprints [4]. The most popular matching methods are based on minutiae representations, where the matching has to pair the different minutiae points. In this context, many works have applied learning-based techniques such as SVMs [52], while fuzzy systems have been used to cope with nonlinear distortions [53]. In addition, CI approaches that do not rely on minutiae, but on the full image, are providing promising results [79].

In iris recognition, the features are usually coded using binary strings, and therefore the adoption of simple matching methods, such as Hamming distance, is common [80]. Nonetheless, many researchers have used CI techniques to perform iris matching [81], especially with non-ideal images. For instance, the work in [48] uses deep learning to match heterogeneous irises, while the work in [51] employs SVMs to improve the performance using images captured in an uncontrolled scenario.

3.7 CLASSIFICATION

In biometric systems, classification methods are used to partition the set of biometric samples in several classes, so that the matching is performed considering only the samples belonging to the same class, thus reducing the computational time required for the recognition.

In fingerprint recognition, the most used classification method is the PCASYS [58], and is based on neural classifiers. Moreover, the work proposed in [54] compares the neural and SVM classifiers using features based on Gabor filtering. Furthermore, the method described in [55] uses neural networks to classify fingerprints by evaluating pseudo-Zernike moments. Genetic algorithms are used in [82] to learn a set of features that possess the most discriminatory information.

In face recognition systems, the method proposed in [56] uses CNNs for classifying face regions in an image based on their importance.

In iris recognition, the work proposed in [57] uses PCA and neural networks to analyze the entropy of iris images, and classify the samples in six categories.

3.8 MULTIBIOMETRIC SYSTEMS

Multibiometric systems can use multiple acquisition sensors, recognition algorithms, biometric samples, or biometric traits (e.g., face and voice) to enhance the recognition accuracy of biometric systems [83].

Multibiometric technologies present important advantages over traditional biometric systems [84], such as robustness to problems due to the non-universality of biometric traits (some people cannot use a certain biometric trait), robustness to spoof attacks and noisy data, and increased fault tolerance.

In order to obtain a single decision from the different modules composing multibiometric systems, it is necessary to perform an additional information fusion step with respect to traditional biometric technologies. This step presents challenges due to the use of heterogeneous data characterized by different amounts of discriminative characteristics and noise. Therefore, many studies in the literature use CI techniques to robustly perform the information fusion by learning the characteristics of the considered source of data and reduce noise.

Multibiometric systems can perform the information fusion at different levels: sensor-level, feature-level, score-level, rank-level, decision-level:

- *Sensor-level*: the raw biometric data are fused to obtain a more discriminative sample and reduce the noise. CI techniques are applied to obtain robust sample representations by overcoming differences in the raw biometric data due to noise, user movements and environmental conditions. For example, the study described in [59] uses neural networks to compute three-dimensional face models from multiple face images, while the method presented in [85] uses genetic algorithms to optimize the fusion of face images acquired in visible light and infrared illumination.
- *Feature-level*: feature vectors obtained from different feature extraction algorithms are fused to create a single template. However, the feature vectors can be related to different biometric traits and present strong differences in data type. CI techniques are frequently used to search the most discriminative characteristics, reduce the dimensionality of the template and optimize fusion strategies. Learning method like SVM are widely used in adaptive biometric systems to perform template updates [60]. Genetic algorithms are also used to optimize fusion methods at the feature level [86].

- *Score-level*: the match scores obtained by multiple matchers are fused to obtain a single match score. Supervised learning techniques are widely used to learn the relationship between the vector of match scores and compute the final match score [61]. Other approaches are based on fuzzy logic [62] and genetic algorithms [87].
- *Rank level*: for each matcher, the ranking is computed from a set of all the possible matching identities sorted in decreasing order of confidence. Most of the methods in the literature are based on statistical approaches [84].
- *Decision-level*: the final “yes/no” decisions of different matchers are fused. This approach is usually adopted in the cases in which it is not possible to modify existing biometric algorithms to obtain other information. Most of the methods in the literature are based on voting strategies, but there are also methods based on optimization techniques, like swarm optimization [88].

3.9 SCORE NORMALIZATION

In the literature, there are studies that aim at increasing the accuracy of biometric systems by post-processing the raw matching scores obtained by the recognition system. The majority of these methods use supervised learning techniques, like SVM, to learn and optimize the distributions of imposters and genuines from training datasets. In particular, there are techniques that estimate normalization functions from both genuines and impostors [89], cohort normalization strategies that evaluate only the impostor distribution [63], and methods that classify the matching scores according to the Doddington Zoo [64].

3.10 ANTISPOOFING

Spoofing attacks consist of the submission of a fake biometric to the sensor, e.g., a fake finger, a face photography or a contact lens with a printed iris pattern. The implementation of anti-spoofing methods that detect the liveness of the biometric sample is an important measure to guarantee the security of biometric systems [90].

Regarding face recognition, most systems operate on 2D images, which may be attacked using photos, videos, make-up, masks, or mannequin heads [91]. In order to avoid these attacks, the work in [66] uses SVMs to analyze the motion, under the assumption that a 2D object moves differently from a real 3D face. Moreover, SVMs are used in [69] to analyze the texture pattern of the image, and in [67] to detect lip movements.

Fingerprint recognition systems can be attacked using fake fingers created using gelatin, silicone or other materials, as well as with dead fingers [92]. Several techniques have tried to detect these attacks by exploiting texture differences between real and fake fingerprints, by using methods such as fuzzy systems [72] or SVMs [70]. Other methods try to detect vital signs, for example using neural networks to analyze pore perspiration [65].

Iris recognition systems can be deceived using methods like artificial eyes, printed iris images, contact lenses or displays [93]. Some techniques that prevent these attacks aim at detecting physiological characteristics, like eye motion or pupillary contraction, using SVMs [68]. SVM classifiers are also used in [71] to distinguish fake and real irises based on their optical characteristics under different lighting conditions.

3.11. PRIVACY

Biometric systems, with respect to traditional recognition methods, offer an increased confidence that the person is actually who he claims to be [94]. However, the consequences of a misuse of biometric information can be dangerous, as in the case of the theft of biometric data [94, 95]. This problem is a common fear for many people, who think that their data are improperly used to track their activities. Hence, it is important to design privacy-compliant biometric systems, taking into account factors related to both technological and sociological aspects [96, 97].

In this context, CI techniques are often used [98] because they offer the possibility to achieve strong encryption and high accuracy [73]. In particular, privacy-preserving biometric recognition methods have been proposed using SVMs [73] and neural networks [73, 74].

4. CONCLUSIONS

Biometric systems are being increasingly used for the recognition of individuals in security applications. The design of such systems, however, requires tackling different technological areas at the same time by dealing with all aspects in an integrated way.

In this context, Computational Intelligence (CI) plays a key role, because it provides the opportunity to design adaptable and evolvable systems, tolerant to incomplete and imprecise data.

This paper has reviewed recent advances in this field, presenting CI techniques that cover all the steps of biometric recognition, including acquisition, segmentation, quality assessment, enhancement, feature extraction, matching, classification, multibiometric fusion, score normalization, antispoofing, and privacy protection.

The proposed review showed that CI techniques are enabling technologies for increasing the accuracy and robustness to non-idealities with respect to traditional algorithmic approaches, and that different CI approaches can be successfully used to perform all the tasks of the biometric recognition process. In particular, we think that recent techniques like deep learning and Convolutional Neural Networks (CNN) will be increasingly studied in the near future in order to further increase the performance of current biometric systems.

ACKNOWLEDGEMENTS

This work was supported in part by the EC within the 7FP under grant agreement 312797 (ABC4EU); the EC within the H2020 program under grant agreement 644597 (ESCUDO-CLOUD); and the Italian Ministry of Research within the project “GenData 2020” (2010RTFWBH).

5. REFERENCES

[1] A. K. Jain, P. Flynn and A. A. Ross, Handbook of biometrics, Springer, 2007.

[2] V. Piuri, F. Scotti and R. Donida Labati, Touchless fingerprint biometrics, CRC Press, 2015.

[3] A. Genovese, V. Piuri and F. Scotti, Touchless palmprint recognition systems, Springer, 2014.

[4] D. Maltoni, D. Maio, A. K. Jain and S. Prabhakar, Handbook of Fingerprint Recognition, 2nd edition ed., Springer, 2009.

[5] A. P. Engelbrecht, Computational intelligence: an introduction, John Wiley & Sons, 2007.

[6] C. Alippi, A. Ferrero and V. Piuri, "Artificial intelligence for instruments and measurement applications," *IEEE Instrumentation & Measurement Magazine*, vol. 1, no. 2, pp. 9-17, 1998.

[7] S. S. Haykin, Neural networks and learning machines, 3rd edition ed., Prentice Hall, 2009.

[8] C. Campbell, "An introduction to kernel methods," in *Studies in Fuzziness and Soft Computing*, vol. 66, Springer, 2001, pp. 155-192.

[9] E. Trillas and L. Eciolaza, Fuzzy Logic, Springer, 2015.

[10] Y.-F. Wang, E. Y. Chang and K. P. Cheng, "A video analysis framework for soft biometry security surveillance," in *Proc. of VSSN '05*, 2005.

[11] H. A. Rowley, S. Baluja and T. Kanade, "Neural network-based face detection," *IEEE Trans. On Pattern Analysis and Machine Intelligence*, pp. 23-38, 1998.

[12] H. Li, Z. Lin, X. Shen, J. Brandt and G. Hua, "A convolutional neural network cascade for face detection," in *Proc. of CVPR 2015*, 2015.

[13] C.-F. Juang and S.-J. Shiu, "Using self-organizing fuzzy network with support vector learning for face detection in color images," *Neurocomputing*, pp. 3409-3420, 2008.

[14] O. Çeliktutan, S. Ulukaya and B. Sankur, "A comparative study of face landmarking techniques," *EURASIP Journal on Image and Video Processing*, vol. 13, 2013.

[15] E. Zhu, J. Yin, C. Hu and G. Zhang, "A systematic method for fingerprint ridge orientation estimation and image segmentation," *Pattern Recognition*, vol. 39, no. 8, pp. 1452-1472, 2006.

[16] A. C. P. Barreto-Marques and A. C. Gay-Thome, "A neural network fingerprint segmentation method," in *Proc. of HIS'05*, 2005.

[17] V. Piuri, F. Scotti and R. Donida Labati, "Neural-based iterative approach for iris detection in iris recognition systems," in *Proc. of CISDA 2009*, 2009.

[18] F. Scotti and V. Piuri, "Adaptive Reflection Detection and Location in Iris Biometric Images by Using Computational Intelligence Techniques," *IEEE Trans. on Instrumentation and Measurement*, vol. 59, no. 7, pp. 1825-1833, 2010.

[19] F. Scotti, "Computational intelligence techniques for reflections identification in iris biometric images," in *Proc. of CIMSA 2007*, 2007.

[20] T. Rongnian and W. Shaojie, "Improving iris segmentation performance via borders recognition," in *Proc. of ICICTA 2011*, 2011.

[21] J. Kang and W. Zhang, "Fingerprint image segmentation using modified fuzzy c-means algorithm," in *Proc. of ICBBE 2009*, 2009.

[22] H. Proenca and L. Alexandre, "Iris segmentation methodology for non-cooperative recognition," *IEEE Proc. on Vision, Image and Signal Processing*, vol. 153, no. 2, pp. 199-205, 2006.

[23] R. Donida Labati, A. Genovese, E. Muñoz, V. Piuri, F. Scotti and G. Sforza, "Automatic Classification of Acquisition Problems Affecting Fingerprint Images in Automated Border Controls," in *Proc. of SSCI 2015*, 2015.

[24] N. A. Schmid, J. Zuo, F. Nicolo and H. Wechsler, "Iris Quality Metrics for Adaptive Authentication," in *Handbook of Iris Recognition*, M. J. Burge and K. W. Bowyer, Eds., Springer, 2013, p. 67–84.

[25] E. Tabass, C. W. and C. Watson, "NIST Fingerprint image quality," NIST, 2004.

[26] M. A. Olsen, E. Tabassi, A. Makarov and C. Busch, "Self-Organizing Maps for Fingerprint Image Quality Assessment," in *Proc. of CVPRW 2013,* 2013.

[27] R. Donida Labati, V. Piuri and F. Scotti, "Neural-based quality measurement of fingerprint images in contactless biometric systems," in *Proc. of IJCNN 2010,* 2010.

[28] R. Donida Labati, A. Genovese, V. Piuri and F. Scotti, "Quality measurement of unwrapped three-dimensional fingerprints: A neural networks approach," in *Proc. of IJCNN 2012,* 2012.

[29] J. R. Beveridge, D. S. Bolme, B. A. Draper, G. H. Givens, Y. M. Lui and P. J. Phillips, "Quantifying how lighting and focus affect face recognition performance," in *Proc. of CVPRW 2010,* 2010.

[30] B. F. Klare and A. K. Jain, "Face recognition: Impostor-based measures of uniqueness and quality," in *Proc. of BTAS 2012,* 2012.

[31] S. Bharadwaj, M. Vatsa and R. Singh, "Can holistic representations be used for face biometric quality assessment?," in *Proc. of ICIP 2013*, 2013.

[32] D. Gragnaniello, C. Sansone and L. Verdoliva, "Iris liveness detection for mobile devices based on local descriptors," *Pattern Recognition Letters,* vol. 57, p. 81–87, 2015.

[33] J. Jang, K. R. Park, J. Kim and Y. Lee, "New focus assessment method for iris recognition systems," *Pattern Recognition Letters,* vol. 29, no. 13, pp. 1759-1767, 2008.

[34] M. Sahasrabudhe and A. M. Namboodiri, "Fingerprint enhancement using unsupervised hierarchical feature learning," in *Proc. of ICVGIP '14,* 2014.

[35] L. Ji, Z. Yi, L. Shang and X. Pu, "Binary fingerprint image thinning using template-based PCNNs," *IEEE Trans. on Systems, Man, and Cybernetics, Part B (Cybernetics),* vol. 37, no. 5, pp. 1407-1413, 2007.

[36] R. Donida Labati, A. Genovese, V. Piuri and F. Scotti, "Contactless fingerprint recognition: A neural approach for perspective and rotation effects reduction," in *Proc. of CIBIM 2013,* 2013.

[37] R. Donida Labati, A. Genovese, V. Piuri and F. Scotti, "Measurement of the principal singular point in contact and contactless fingerprint images by using computational intelligence techniques," in *Proc. of CIMSA 2010*, 2010.

[38] K. Cao and A. K. Jain, "Latent orientation field estimation via convolutional neural network," in *Proc. of ICB 2015,* 2015.

[39] M. Song, D. Tao, X. Huang, C. Chen and J. Bu, "Three-dimensional face reconstruction from a single image by a coupled RBF Network," *IEEE Trans. on Image Processing,* vol. 21, no. 5, pp. 2887-2897, 2012.

[40] S. H. Moi, H. Asmuni, R. Hassan and R. M. Othman, "A unified approach for unconstrained off-angle iris recognition,," in *Proc. of ISBAST 2014,* 2014.

[41] G. Xu, Z. Zhang and Y. Ma, "A novel method for iris feature extraction based on intersecting cortical model network," *Journal of Applied Mathematics and Computing,* vol. 26, no. 1, pp. 341-352, 2005.

[42] A. Genovese, E. Muñoz, V. Piuri, F. Scotti and G. Sforza, "Towards touchless pore fingerprint biometrics: a neural approach," in *Proc. of IJCNN 2016*, 2016.

[43] S. Gao, Y. Zhang, K. Jia, J. Lu and Y. Zhang, "Single sample face recognition via learning deep supervised autoencoders," *IEEE Trans. on Information Forensics and Security,* vol. 10, no. 10, pp. 2108-2118, 2015.

[44] C. Ding and D. Tao, "Robust face recognition via multimodal deep face representation," *IEEE Trans. on Multimedia,* vol. 17, no. 11, pp. 2049-2058, 2015.

[45] C. Xiong, L. Liu, X. Zhao, S. Yan and T. K. Kim, "Convolutional fusion network for face verification in the wild," *IEEE Trans. on Circuits and Systems for Video Technology,* vol. 26, no. 3, pp. 517-528, 2016.

[46] J. Zhang, S. Shan, M. Kan and X. Chen, "Coarse-to-Fine Auto-Encoder Networks (CFAN) for Real-Time Face Alignment," in *Proc. of ECCV 2014,* 2014.

[47] Y. Sun, X. Wang and X. Tang, "Hybrid Deep Learning for Face Verification," in *Proc. of ICCV 2013,* 2013.

[48] N. Liu, M. Zhang, H. Li, Z. Sun and T. Tan, "DeepIris: Learning pairwise filter bank for heterogeneous iris verification," *Pattern Recognition Letters,* 2015.

[49] A. Asthana, S. Zafeiriou, S. Cheng and M. Pantic, "Incremental Face Alignment in the Wild," in *Proc. of CVPR 2014*, 2014.

[50] X. Song, Y. Zheng, X. Wu, X. Yang and J. Yang, "A complete fuzzy discriminant analysis approach for face recognition," *Applied Soft Computing,* vol. 10, no. 1, pp. 208-214, 2010.

[51] K. Roy and P. Bhattacharya, "Level Set Approaches and Adaptive Asymmetrical SVMs Applied for Nonideal Iris Recognition," in *Image Analysis and Recognition*, M. K. and A. Campilho, Eds., Springer, 2009, pp. 418-428.

[52] P. Mansukhani and V. Govindaraju, "Selecting optimal classification features for SVM based elimination of incorrectly matched minutiae," in *Proc. of SPIE 6944, Biometric Technology for Human Identification V*, 2008.

[53] X. Chen, J. Tian and X. Yang, "A new algorithm for distorted fingerprints matching based on normalized fuzzy similarity measure," *IEEE Trans. on Image Processing,* vol. 15, no. 3, pp. 767-776, 2006.

[54] T. Kristensen, J. Borthen and K. Fyllingsnes, "Comparison of neural network based fingerprint classification techniques," in *Proc. of IJCNN 2007*, 2007.

[55] I. El-Feghi, A. Tahar and M. Ahmadi, "Efficient features extraction for fingerprint classification with multilayer perceptron neural network," in *Proc. of ISSCS 2011*, 2011.

[56] S. Kang, D. Lee and C. D. Yoo, "Face attribute classification using attribute-aware correlation map and gated convolutional neural networks," in *Proc. of ICIP 2015*, 2015.

[57] L. Nasseri, A. A. B. Shirazi and N. Sadeghigol, "Tsallis entropy, PCA and neural network in novel algorithm of iris classification," in *Proc. of WICT 2011*, 2011.

[58] G. T. Candela, P. J. Grother, C. I. Watson, R. A. Wilkinson and C. L. Wilson, "PCASYS - A Pattern-Level Classification Automation System for Fingerprints," NIST Internal Report - 5647, 1995.

[59] M. I. Fanany, M. Ohno and I. Kumazawa, "A scheme for reconstructing face from shading using smooth projected polygon representation NN," in *Proc. of ICIP 2002*, 2002.

[60] A. Rattani, F. Roli and E. Granger, Adaptive Biometric Systems, Springer, 2015.

[61] M. He, S.-J. Horng, P. Fan, R.-S. Run, R.-J. Chen, J.-L. Lai, M. K. Khan and K. O. Sentosa, "Performance evaluation of score level fusion in multimodal biometric systems," *Pattern Recognition,* vol. 43, no. 5, pp. 1789 - 1800, May 2010.

[62] F. Scotti, A. Azzini, S. Marrara and R. Sassi, "A fuzzy approach to multimodal biometric continuous authentication," *Fuzzy Optimization and Decision Making,* pp. 243-256, September 2008.

[63] N. Poh, M. Tistarelli and Y. Sun, "On the Use of Discriminative Cohort Score Normalization for Unconstrained Face Recognition," *IEEE Trans. on Information Forensics and Security,* vol. 9, no. 12, pp. 2063 - 2075, December 2014.

[64] N. Poh and J. Kittler, "Incorporating Model-Specific Score Distribution in Speaker Verification Systems," *IEEE Trans. on Audio, Speech, and Language Processing,* vol. 16, no. 3, pp. 594 - 606, March 2008.

[65] B. Tan and S. Schuckers, "Spoofing protection for fingerprint scanner by fusing ridge signal and valley noise," *Pattern Recognition,* vol. 43, no. 8, pp. 2845-2857, 2010.

[66] K. Kollreider, H. Fronthaler and J. Bigun, "Non-intrusive liveness detection by face images," *Image and Vision Computing,* vol. 27, no. 3, pp. 233-244, 2009.

[67] K. Kollreider, H. Fronthaler, M. I. Faraj and J. Bigun, "Real-Time Face Detection and Motion Analysis With Application in Liveness Assessment," *IEEE Trans. on Information Forensics and Security,* vol. 2, no. 3, pp. 548-558, 2007.

[68] X. Huang, C. Ti, Q.-z. Hou, A. Tokuta and R. Yang, "An experimental study of pupil constriction for liveness detection," in *Proc. of WACV 2013*, 2013.

[69] J. Määttä, A. Hadid and M. Pietikainen, "Face spoofing detection from single images using micro-texture analysis," in *Proc. of IJCB 2011*, 2011.

[70] A. Rattani and A. Ross, "Automatic adaptation of fingerprint liveness detector to new spoof materials," in *Proc. of IJCB 2014*, 2014.

[71] R. Chen, X. Lin and T. Ding, "Liveness detection for iris recognition using multispectral images," *Pattern Recognition Letters,* vol. 33, no. 12, pp. 1513-1519, 2012.

[72] A. Schuckers and S. Abhyankar, "Fingerprint Liveness Detection Using Local Ridge Frequencies and Multiresolution Texture Analysis Techniques," in *Proc. of ICIP 2006,* 2006.

[73] M. Upmanyu, A. M. Namboodiri, K. Srinathan and C. V. Jawahar, "Blind Authentication: A Secure Crypto-Biometric Verification Protocol," *IEEE Trans. on Information Forensics and Security,* vol. 5, no. 2, pp. 255-268, 2010.

[74] M. Barni, P. Failla, R. Lazzeretti, A. R. Sadeghi and T. Schneider, "Privacy-Preserving ECG Classification With Branching Programs and Neural Networks," *IEEE Trans. on Information Forensics and Security,* vol. 6, no. 2, pp. 452-

468, 2011.

[75] S. Z. Li and A. K. Jain, Handbook of Face Recognition, Springer, 2011.

[76] R. Donida Labati, A. Genovese, V. Piuri and F. Scotti, "Iris segmentation: state of the art and innovative methods," in *Cross Disciplinary Biometric Systems*, vol. 37, C. Liu and V. Mago, Eds., Springer, 2012, pp. 151-182.

[77] M. Gamassi, M. Lazzaroni, M. Misino, V. Piuri, D. Sana and F. Scotti, "Quality assessment of biometric systems: a comprehensive perspective based on accuracy and performance measurement," *IEEE Trans. on Instrumentation and Measurement*, pp. 1489-1496, 2005.

[78] F. Alonso-Fernandez, J. Fierrez and J. Ortega-Garcia, "Quality Measures in Biometric Systems," *IEEE Security Privacy*, vol. 10, no. 6, pp. 52-62, 2012.

[79] L. Lumini and A. Nanni, "Descriptors for image-based fingerprint matchers," *Expert Systems with Applications*, vol. 36, no. 10, pp. 12414-12422, 2009.

[80] W. Dong, Z. Sun and T. Tan, "Iris Matching Based on Personalized Weight Map," *IEEE Trans. on Pattern Analysis and Machine Intelligence*, vol. 33, no. 9, pp. 1744-1757, 2011.

[81] M. De Marsico, A. Petrosino and S. Ricciardi, "Iris Recognition through Machine Learning Techniques: a Survey," *Pattern Recognition Letters,* 2016.

[82] X. Tan, B. Bhanu and Y. Lin, "Fingerprint classification based on learned features," *IEEE Trans. on Systems, Man, and Cybernetics, Part C (Applications and Reviews)*, vol. 35, no. 3, pp. 287-300, 2005.

[83] A. Ross, "Multibiometrics," in *Encyclopedia of Cryptography and Security, Second Edition*, C. A. Henk and S. Jajodia, Eds., Springer, 2011, pp. 967 - 973.

[84] A. Ross, A. K. Jain and K. Nandakumar, Handbook of Multibiometrics, Springer, 2006.

[85] S. Singh, A. Gyaourova, G. Bebis and I. Pavlidis, "Infrared and Visible Image Fusion for Face Recognition," in *Proc. of SPIE 5404*, 2004.

[86] N. K. Ratha and A. K. Jain, "Infrared and Visible Image Fusion for Face Recognition," in *Proc. of SPIE 5404*, 2004.

[87] N. Alajlan, N. Ammour and M. S. Islam, "Fusion of fingerprint and heartbeat biometrics using fuzzy adaptive genetic algorithm," in *Proc. of WCIS 2013*, 2013.

[88] N. Srinivas, K. Veeramachaneni, L. Osadciw and A. Ross, "Decision-level Fusion Strategies for Correlated Biometric Classifiers," in *Proc. of CVPRW 2008*, 2008.

[89] A. Ross, A. Jain and K. Nandakumar, "Score normalization in multimodal biometric systems," *Pattern Recognition*, vol. 38, no. 12, pp. 2270- 2285, December 2005.

[90] R. Donida Labati, A. Genovese, E. Muñoz, F. Scotti, V. Piuri and G. Sforza, "Advanced design of Automated Border Control gates: biometric system techniques and research trends," in *Proc. of ISSE 2015*, 2015.

[91] O. Kähm and N. Damer, "2D face liveness detection: An overview," in *Proc. of BIOSIG 2012*, 2012.

[92] E. Marasco and A. Ross, "A survey on antispoofing schemes for fingerprint recognition systems," *ACM Computing Surveys*, vol. 47, no. 2, pp. 1-36, 2014.

[93] H. Wei, L. Chen and J. Ferryman, "Biometrics in ABC: Counter-Spoofing Research," in *Proc. of the Frontex Global Conference on Future Developments of Automated Border Control*, 2013.

[94] R. Donida Labati, V. Piuri and F. Scotti, "Biometric privacy protection: guidelines and technologies," in *E-Business and Telecommunications*, Springer, 2012, pp. 3-19.

[95] S. Cimato, M. Gamassi, V. Piuri, R. Sassi and F. Scotti, "Privacy-Aware Biometrics: Design and Implementation of a Multimodal Verification System," in *Proc. of ACSAC 2008*, 2008.

[96] V. Ciriani, S. De Capitani di Vimercati, S. Foresti and P. Samarati, "Microdata Protection," in *Secure Data Management in Decentralized Systems*, T. Yu and S. Jajodia, Eds., Springer, 2007, pp. 291-321.

[97] S. De Capitani di Vimercati, S. Foresti, G. Livraga and P. Samarati, "Data privacy: definitions and techniques," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 20, no. 6, pp. 793-817, 2012.

[98] M. Barni, T. Bianchi, D. Catalano, M. Di Raimondo, R. Donida Labati, P. Failla, D. Fiore, R. Lazzeretti, V. Piuri and A. Piva, "A privacy-compliant fingerprint recognition system based on homomorphic encryption and fingercode templates," in *Proc. of BTAS 2010*, 2010.